EVOLUTION OF COMPUTER VIRUSES

	First Generation	Second Generation
Language	Assembly language	Scripting language
Distribution Form	Binary	Source
Host Platform	CPU and OS	Source
Host Object	Executable codes	Documents
Propagation Media	Physical media	Network

FIG. 1
(PRIOR ART)

VIRUS DETECTION AND IDENTIFICATION

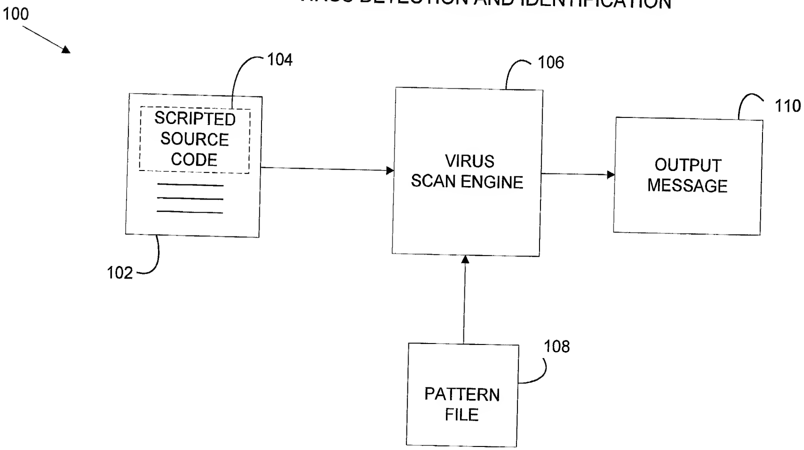

FIG. 2
(PRIOR ART)

SCRIPTING VIRUS SCAN ENGINE

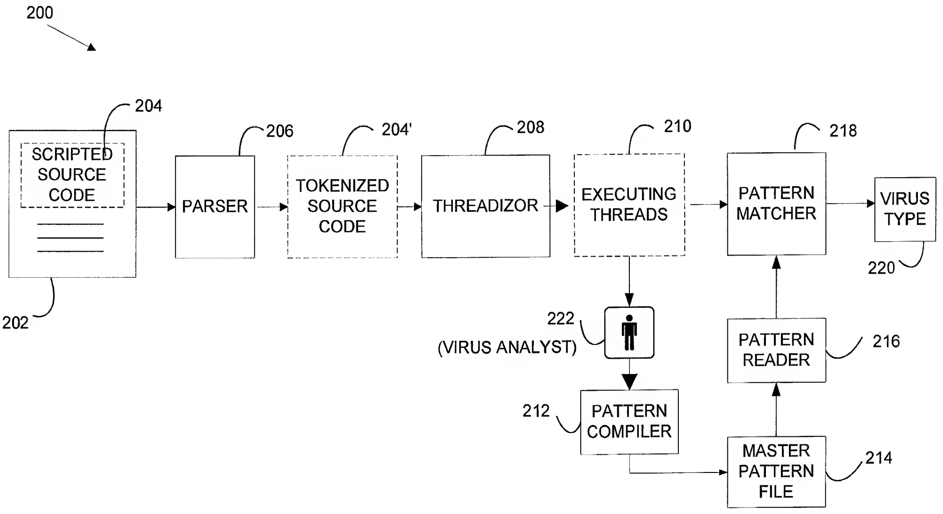

FIG. 3

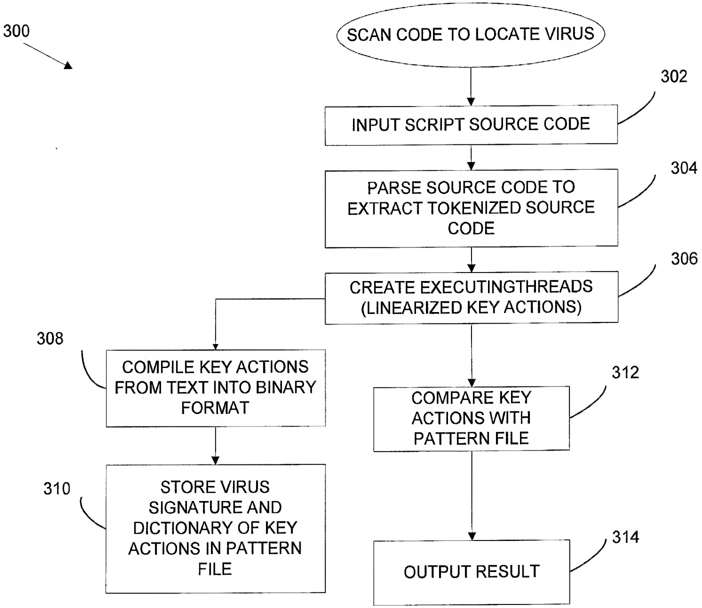
300
SCAN CODE TO LOCATE VIRUS
302
INPUT SCRIPT SOURCE CODE
304
PARSE SOURCE CODE TO EXTRACT TOKENIZED SOURCE CODE
306
CREATE EXECUTINGTHREADS (LINEARIZED KEY ACTIONS)
308
COMPILE KEY ACTIONS FROM TEXT INTO BINARY FORMAT
310
STORE VIRUS SIGNATURE AND DICTIONARY OF KEY ACTIONS IN PATTERN FILE
312
COMPARE KEY ACTIONS WITH PATTERN FILE
314
OUTPUT RESULT

FIG. 4

SCRIPT SOURCE CODE

```
Private fso
Sub   F1
Set file =fso . OpenTextFile ("your bank account", ForReading, True)
str = file .  ReadLine
file . Close   (     )
End     Sub

Sub     F2
Set file =fso . CreateTextFile ("c:\autoexec.bat", True )
file .  WriteLine ("format c:" )
file     .     Close     (     )
End     Sub


On Error      Resume      Next
Set fso=CreateObject  ("Scripting.FileSystemObject" )
Call     F1
Call     F2
```

FIG. 5A

TOKENIZED SOURCE CODE

```
Private fso
Sub    F1
Set file = fso . OpenTextFile ( "your bank account" ,  ForReading , True )
str = file .  ReadLine
file . Close    (    )
End     Sub

Sub     F2
Set file = fso . CreateTextFile ( "c:\autoexec.bat" , True   )
file . WriteLine  ( "format c:"  )
file    .     Close     (     )
End     Sub


On Error      Resume     Next
Set fso = CreateObject  ( "Scripting.FileSystemObject" )
Call     F1
Call     F2
```

FIG. 5B

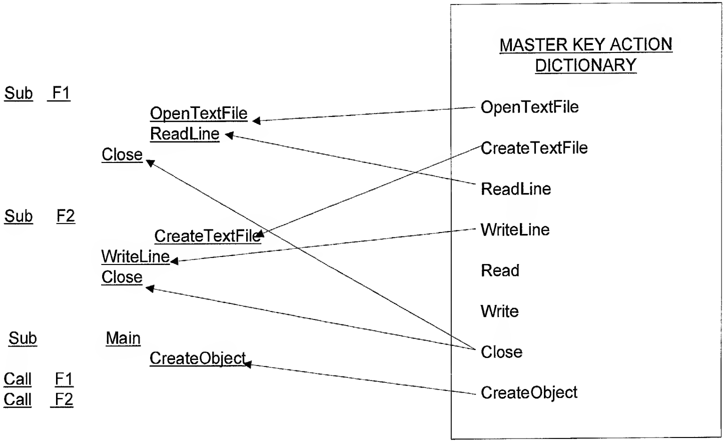
Sub F1
OpenTextFile
ReadLine
Close
Sub F2
CreateTextFile
WriteLine
Close
Sub Main
CreateObject
Call F1
Call F2
MASTER KEY ACTION DICTIONARY
OpenTextFile
CreateTextFile
ReadLine
WriteLine
Read
Write
Close
CreateObject

FIG. 6

LINEARIZED KEY ACTIONS

```
Sub   Main

        CreateObject
        OpenTextFile
        ReadLine
        Close
        CreateTextFile
        WriteLine
        Close
```

FIG. 7

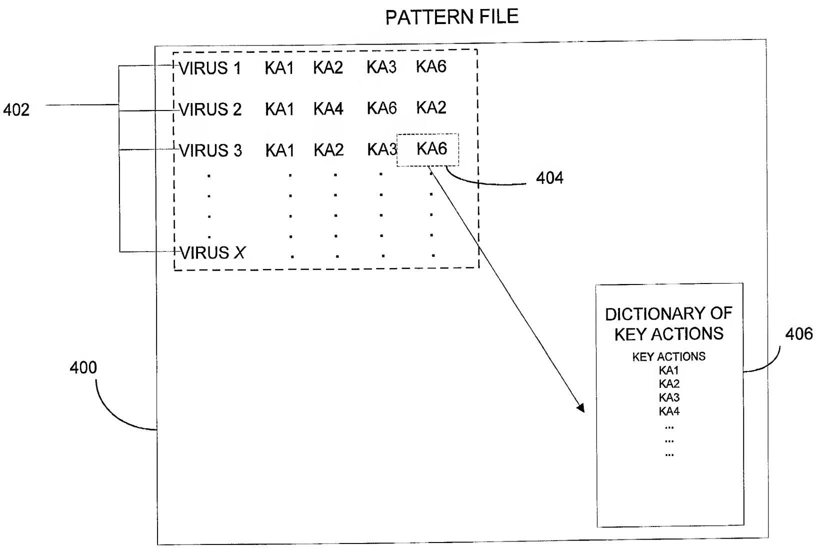
PATTERN FILE
VIRUS 1 KA1 KA2 KA3 KA6
VIRUS 2 KA1 KA4 KA6 KA2
VIRUS 3 KA1 KA2 KA3 KA6
VIRUS X
402
404
400
DICTIONARY OF KEY ACTIONS
KEY ACTIONS
KA1
KA2
KA3
KA4
...
...
...
406

FIG. 8

POLYMORPH SCRIPT SOURCE CODE

```
Private obj
Sub    Func2
Set file = obj. CreateTextFile ("c:\autoexec.bat", True )
file .  WriteLine ("format c:" )
file . Close   (     )
End     Sub

Sub     F1
Set file = obj . OpenTextFile ("your bank account", ForReading, True)
str = file .  ReadLine
file     .     Close     (     )
End     Sub


On Error      Resume      Next
Set obj = CreateObject  ("Scripting.FileSystemObject" )
Call     F1
Call     Func2
```

FIG. 9A

TOKENIZED POLYMORPH SOURCE CODE

```
Private obj
Sub     Func2
Set file = obj . CreateTextFile ( "c:\autoexec.bat" , True  )
file . WriteLine  ( "format c:"  )
file . Close   (    )
End     Sub

Sub    F1
Set file = obj . OpenTextFile ( "your bank account" ,  ForReading , True )
str = file .  ReadLine
file   .     Close     (    )
End     Sub

On Error     Resume     Next
Set obj = CreateObject  ( "Scripting.FileSystemObject" )
Call     F1
Call     Func2
```

FIG. 9B

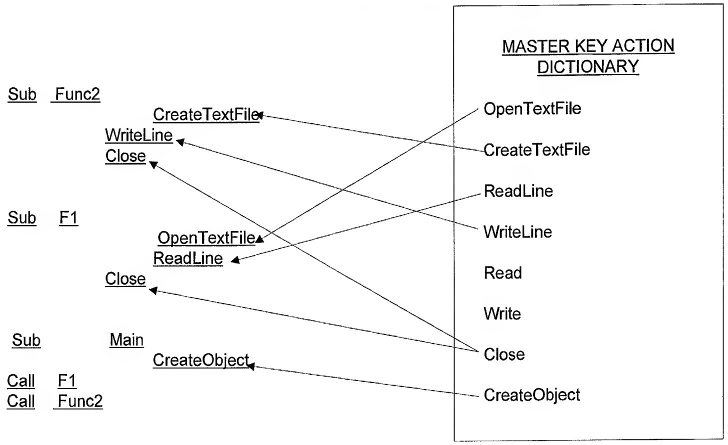
Sub Func2
CreateTextFile
WriteLine
Close
Sub F1
OpenTextFile
ReadLine
Close
Sub Main
CreateObject
Call F1
Call Func2
MASTER KEY ACTION DICTIONARY
OpenTextFile
CreateTextFile
ReadLine
WriteLine
Read
Write
Close
CreateObject

FIG. 10

LINEARIZED KEY ACTIONS OF POLYMORPH

```
Sub   Main

      CreateObject
      OpenTextFile
      ReadLine
      Close
      CreateTextFile
      WriteLine
      Close
```

FIG. 11

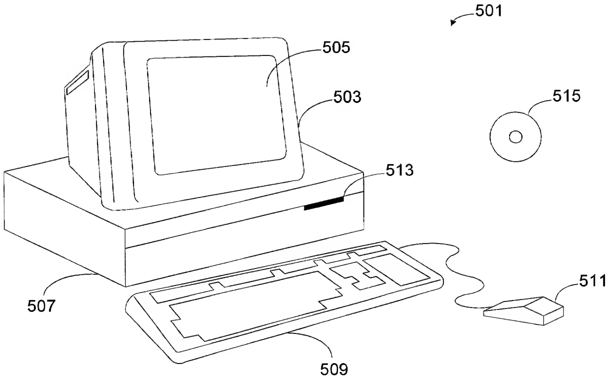

FIG. 12A

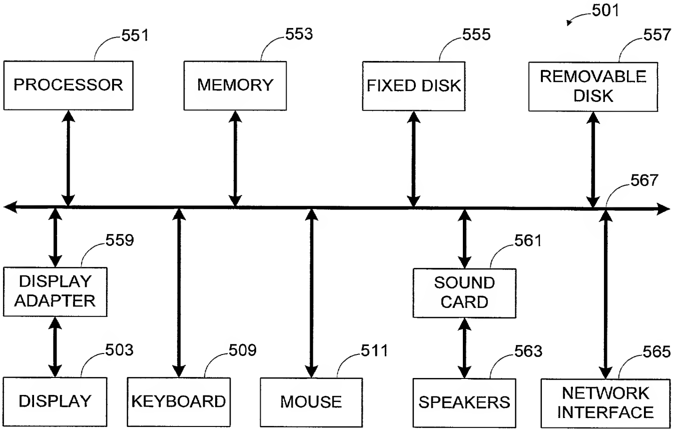

FIG. 12B